UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/810,696	03/29/2004	Masami Nasu	251145US2	1217

22850 7590 09/27/2007

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
LOUIE, OSCAR A	

ART UNIT	PAPER NUMBER
2136	

NOTIFICATION DATE	DELIVERY MODE
09/27/2007	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/810,696	NASU, MASAMI	
	Examiner	Art Unit	
	Oscar A. Louie	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *29 March 2004*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *29 March 2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *08/04*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This first non-final action is in response to the original filing of 03/29/2004. Claims 1-56 are pending and have been considered as follows.

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1, 14, 22, 30, 43, & 50 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

- The term "capable" in claims 1, 14, 22, 30, 43, & 50 is a relative term which renders the claims indefinite. The term "capable" is not defined by the claims, the specification does not provide a standard for ascertaining the requisite degree, and one of ordinary skill in the art would not be reasonably apprised of the scope of the invention.
- The examiner notes that the term "capable" is indefinite as it may render the applicant's invention as inoperable since it is unclear as to whether the applicant's limitations are indeed "capable" of being performed.

Claim Rejections - 35 USC § 101

3. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 22 & 50 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

- Claims 22 & 50 both disclose a program, which is non-statutory as in accordance with 35 U.S.C. 101. The examiner notes that when using claim language, which includes a computer program, the applicant must include disclosure for "a computer readable storage medium" as a part of the claim. The applicant must also clearly have support in their specification as to the scope of the "computer readable storage medium."

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 1-4, 6-9, 12-17, 20-25, 28-32, 35-38, 41-45, 48-52, 55, & 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. (US-7069452-B1) in view of Kidder et al. (US-6880086-B2).

Claim 1:

Hind et al. disclose a software update device capable of communicating with a target update device via a network comprising,

- "a certification information setting unit" (i.e. "A person wishing to receive secure data generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "for generating a first certification information" (i.e. "generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "for transmitting the first certification information to the target update device via a first communication path" (i.e. "The encryption key is made public, while the corresponding decryption key is kept secret") [column 11 lines 29-31];
- "a certification requesting unit" (i.e. "A person wishing to receive secure data generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "for transmitting a second certification information to the target update device" (i.e. "Asymmetric-key cryptosystems may also be used to provide for digital signatures, in which the sender encrypts a signature message using the sender's private key, the signature messing being a hash or message digest of the message being signed") [column 11 lines 35-39];
- "for requesting the target update device to execute a certification process with the first and second certification information" (i.e. "Because the signature message can only be decrypted with the sender's public key, the recipient can use the sender's public key to confirm that the signature message originated with the sender") [column 11 lines 42-45];

- "a transmitting unit for transmitting an update software for updating a software of the target update device to the target update device... when the certification process succeeds" (i.e. "As is seen in FIG. 5, update data may be obtained by providing an "image" of the data to be written to a programmable memory, for example, the programmable memory 14") [column 11 lines 18-20];

but they do not disclose,

- "via a second communication path"
- "the second communication path having a process load less than that of the first communication path"

however, Kidder et al. do disclose,

- "Ethernet 32 provides an out-of-band control path, meaning that control information passes over Ethernet 32 but the network data being switched by computer system 10 passes to and from external network connections 31a-31xx over a separate data path 34" [column 9 lines 14-18];
- "This external network control data is also assigned a high priority when passed over the Ethernet to ensure that it is not dropped during periods of heavy traffic on the Ethernet" [column 9 lines 20-23];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "via a second communication path" and "the second communication path having a process load less than that of the first communication path," in the invention as disclosed by Hind et al. for the purposes of transmitting authentication information and data over separate data paths for ensuring traffic quality of service.

Claim 2:

Hind et al. and Kidder et al. disclose a software update device capable of communicating with a target update device via a network, as in Claim 1 above, further comprising,

- "a certification information invalidation requesting unit for requesting the target update device to invalidate the first certification information subsequent to the transmittal of the update software" (i.e. "If the results do not match, then the signature is not verified (block 406) and the image is rejected, the update procedure terminated and the latch set to disable updates (block 412)") [column 12 lines 52-55].

Claim 3:

Hind et al. and Kidder et al. disclose a software update device capable of communicating with a target update device via a network, as in Claim 1 above, further comprising,

- "the software of the target update device is updated when requested by an external unit" (i.e. "FIG. 5 illustrates operations according to embodiments of the present invention for performing an update of firmware or other data stored in a programmable memory") [column 11 lines 13-15].

Claim 4:

Hind et al. and Kidder et al. disclose a software update device capable of communicating with a target update device via a network, as in Claim 3 above, further comprising,

- "a notification unit for notifying a result of updating the software of the target update device to the external unit" (i.e. "As described above, the candidate image may include a certificate or chain of certificates which may provide a means of verifying a digital signature included with the update image") [column 12 lines 46-49].

Claim 6:

Hind et al. and Kidder et al. disclose a software update device capable of communicating with a target update device via a network, as in Claim 1 above, further comprising,

- "the second communication path is a communication path for communicating by using FTP" (i.e. "an authorized administrator sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 7:

Hind et al. and Kidder et al. disclose a software update device capable of communicating with a target update device via a network, as in Claim 1 above, further comprising,

- "data transmitted via the first communication path is encoded" (i.e. "the image may be digitally signed or otherwise encrypted utilizing, for example, an asymmetric key cryptosystem") [column 11 lines 22-24];
- "data transmitted via the second communication path is not encoded" (i.e. "sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 8:

Hind et al. disclose a software update system comprising,

- "a software update device" [Fig 10 illustrates an updater];
- "a target update device in communication with the software update device" [Fig 10 illustrates an updater in communication with a device to be updated];

- "a certification information setting unit" (i.e. "A person wishing to receive secure data generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "for generating a first certification information" (i.e. "generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "for transmitting the first certification information to a target update device via a first communication path" (i.e. "The encryption key is made public, while the corresponding decryption key is kept secret") [column 11 lines 29-31];
- "a certification requesting unit" (i.e. "A person wishing to receive secure data generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "for transmitting a second certification information to the target update device" (i.e. "Asymmetric-key cryptosystems may also be used to provide for digital signatures, in which the sender encrypts a signature message using the sender's private key, the signature messing being a hash or message digest of the message being signed") [column 11 lines 35-39];
- "for requesting the target update device to execute a certification process with the first and second certification information" (i.e. "Because the signature message can only be decrypted with the sender's public key, the recipient can use the sender's public key to confirm that the signature message originated with the sender") [column 11 lines 42-45];

- "a transmitting unit for transmitting an update software for updating a software of the target update device to the target update device... when the certification process succeeds" (i.e. "As is seen in FIG. 5, update data may be obtained by providing an "image" of the data to be written to a programmable memory, for example, the programmable memory 14") [column 11 lines 18-20];
- "a memory unit for storing the first certification information" [Fig 3 illustrates a memory];
- "a certification unit" [Fig 10 illustrates a device to be updated];
- "for executing the certification process by using the first and second certification information when requested to execute the certification process" (i.e. "Because the signature message can only be decrypted with the sender's public key, the recipient can use the sender's public key to confirm that the signature message originated with the sender") [column 11 lines 42-45];
- "for returning a result of the certification process to the software update device" (i.e. "As described above, the candidate image may include a certificate or chain of certificates which may provide a means of verifying a digital signature included with the update image") [column 12 lines 46-49];
- "an updating unit" [Fig 10 illustrates an updater];
- "for receiving the update software when the certification process succeeds" (i.e. "As is seen in FIG. 5; update data may be obtained by providing an "image" of the data to be written to a programmable memory, for example, the programmable memory 14") [column 11 lines 18-20];

- "for updating the software of the target update device" (i.e. "FIG. 5 illustrates operations according to embodiments of the present invention for performing an update of firmware or other data stored in a programmable memory") [column 11 lines 13-15];

but they do not disclose,

- "via a second communication path"
- "the second communication path having a process load less than that of the first communication path"

however, Kidder et al. do disclose,

- "Ethernet 32 provides an out-of-band control path, meaning that control information passes over Ethernet 32 but the network data being switched by computer system 10 passes to and from external network connections 31a-31xx over a separate data path 34" [column 9 lines 14-18];
- "This external network control data is also assigned a high priority when passed over the Ethernet to ensure that it is not dropped during periods of heavy traffic on the Ethernet" [column 9 lines 20-23];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "via a second communication path" and "the second communication path having a process load less than that of the first communication path," in the invention as disclosed by Hind et al. for the purposes of transmitting authentication information and data over separate data paths for ensuring traffic quality of service.

Claim 9:

Hind et al. disclose a software update system, as in Claim 8 above, further comprising,

- "the software update device further has a certification information invalidation requesting unit for transmitting an invalidation request to invalidate the first certification information to the target update device subsequent to the transmittal of the update software" (i.e. "If the results do not match, then the signature is not verified (block 406) and the image is rejected, the update procedure terminated and the latch set to disable updates (block 412)") [column 12 lines 52-55];
- "the target update device further has a certification information invalidating unit for invalidating the first certification information when receiving the invalidation request" (i.e. "If the results do not match, then the signature is not verified (block 406) and the image is rejected, the update procedure terminated and the latch set to disable updates (block 412)") [column 12 lines 52-55].

Claim 12:

Hind et al. disclose a software update system, as in Claim 8 above, further comprising,

- "the second communication path is a communication path for communicating by using FTP" (i.e. "sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 13:

Hind et al. disclose a software update system, as in Claim 8 above, further comprising,

- "data transmitted via the first communication path is encoded" (i.e. "the image may be digitally signed or otherwise encrypted utilizing, for example, an asymmetric key cryptosystem") [column 11 lines 22-24];
- "data transmitted via the second communication path is not encoded" (i.e. "sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 14:

Hind et al. disclose a software update system comprising,

- "generating a first certification information" (i.e. "A person wishing to receive secure data generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "transmitting the first certification information to the target update device via a first communication path" (i.e. "The encryption key is made public, while the corresponding decryption key is kept secret") [column 11 lines 29-31];
- "transmitting a second certification information to the target update device" (i.e. "Asymmetric-key cryptosystems may also be used to provide for digital signatures, in which the sender encrypts a signature message using the sender's private key, the signature messing being a hash or message digest of the message being signed") [column 11 lines 35-39];

- "requesting the target update device to execute a certification process with the first and second certification information" (i.e. "Because the signature message can only be decrypted with the sender's public key, the recipient can use the sender's public key to confirm that the signature message originated with the sender") [column 11 lines 42-45];
- "transmitting an update software for updating a software of the target update device to the target update device... when the certification process succeeds" (i.e. "As is seen in FIG. 5, update data may be obtained by providing an "image" of the data to be written to a programmable memory, for example, the programmable memory 14") [column 11 lines 18-20];

but they do not disclose,

- "via a second communication path"
- "the second communication path having a process load less than that of the first communication path"

however, Kidder et al. do disclose,

- "Ethernet 32 provides an out-of-band control path, meaning that control information passes over Ethernet 32 but the network data being switched by computer system 10 passes to and from external network connections 31a-31xx over a separate data path 34" [column 9 lines 14-18];
- "This external network control data is also assigned a high priority when passed over the Ethernet to ensure that it is not dropped during periods of heavy traffic on the Ethernet" [column 9 lines 20-23];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "via a second communication path" and "the second communication path having a process load less than that of the first communication path," in the invention as disclosed by Hind et al. for the purposes of transmitting authentication information and data over separate data paths for ensuring traffic quality of service.

Claim 15:

Hind et al. disclose a software update system, as in Claim 14 above, further comprising,

- "a step of requesting the target update device to invalidate the first certification information subsequent to the transmittal of the update software" (i.e. "If the results do not match, then the signature is not verified (block 406) and the image is rejected, the update procedure terminated and the latch set to disable updates (block 412)") [column 12 lines 52-55].

Claim 16:

Hind et al. disclose a software update system, as in Claim 14 above, further comprising,

- "the software of the target update device is updated when requested by an external unit" (i.e. "FIG. 5 illustrates operations according to embodiments of the present invention for performing an update of firmware or other data stored in a programmable memory") [column 11 lines 13-15].

Claim 17:

Hind et al. disclose a software update system, as in Claim 16 above, further comprising,

- "a step of notifying a result of updating the software of the target update device to the external unit" (i.e. "As described above, the candidate image may include a certificate or chain of certificates which may provide a means of verifying a digital signature included with the update image") [column 12 lines 46-49].

Claim 20:

Hind et al. disclose a software update system, as in Claim 14 above, further comprising,

- "the second communication path is a communication path for communicating by using FTP" (i.e. "sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 21:

Hind et al. disclose a software update system, as in Claim 14 above, further comprising,

- "data transmitted via the first communication path is encoded" (i.e. "the image may be digitally signed or otherwise encrypted utilizing, for example, an asymmetric key cryptosystem") [column 11 lines 22-24];
- "data transmitted via the second communication path is not encoded" (i.e. "sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 22:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network comprising,

- "a generating function for generating a first certification information" (i.e. "A person wishing to receive secure data generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "a transmitting function for transmitting the first certification information to the target update device via a first communication path" (i.e. "The encryption key is made public, while the corresponding decryption key is kept secret") [column 11 lines 29-31];
- "a transmitting function for transmitting a second certification information to the target update device" (i.e. "Asymmetric-key cryptosystems may also be used to provide for digital signatures, in which the sender encrypts a signature message using the sender's private key, the signature messing being a hash or message digest of the message being signed") [column 11 lines 35-39];
- "a requesting function for requesting the target update device to execute a certification process with the first and second certification information" (i.e. "Because the signature message can only be decrypted with the sender's public key, the recipient can use the sender's public key to confirm that the signature message originated with the sender") [column 11 lines 42-45];

- "a transmitting function for transmitting an update software for updating a software of the target update device to the target update device... when the certification process succeeds" (i.e. "As is seen in FIG. 5, update data may be obtained by providing an "image" of the data to be written to a programmable memory, for example, the programmable memory 14") [column 11 lines 18-20];

but they do not disclose,

- "via a second communication path"
- "the second communication path having a process load less than that of the first communication path"

however, Kidder et al. do disclose,

- "Ethernet 32 provides an out-of-band control path, meaning that control information passes over Ethernet 32 but the network data being switched by computer system 10 passes to and from external network connections 31a-31xx over a separate data path 34" [column 9 lines 14-18];
- "This external network control data is also assigned a high priority when passed over the Ethernet to ensure that it is not dropped during periods of heavy traffic on the Ethernet" [column 9 lines 20-23];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "via a second communication path" and "the second communication path having a process load less than that of the first communication path," in the invention as disclosed by Hind et al. for the purposes of transmitting authentication information and data over separate data paths for ensuring traffic quality of service.

Claim 23:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, as in Claim 22 above, further comprising,

- "a function of requesting the target update device to invalidate the first certification information subsequent to the transmittal of the update software" (i.e. "If the results do not match, then the signature is not verified (block 406) and the image is rejected, the update procedure terminated and the latch set to disable updates (block 412)") [column 12 lines 52-55].

Claim 24:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, as in Claim 22 above, further comprising,

- "the software of the target update device is updated when requested by an external unit" (i.e. "FIG. 5 illustrates operations according to embodiments of the present invention for performing an update of firmware or other data stored in a programmable memory") [column 11 lines 13-15].

Claim 25:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, as in Claim 24 above, further comprising,

- "a step of notifying a result of updating the software of the target update device to the external unit" (i.e. "As described above, the candidate image may include a certificate or chain of certificates which may provide a means of verifying a digital signature included with the update image") [column 12 lines 46-49].

Claim 28:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, as in Claim 22 above, further comprising,

- "the second communication path is a communication path for communicating by using FTP" (i.e. "sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 29:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, as in Claim 22 above, further comprising,

- "data transmitted via the first communication path is encoded" (i.e. "the image may be digitally signed or otherwise encrypted utilizing, for example, an asymmetric key cryptosystem") [column 11 lines 22-24];

- "data transmitted via the second communication path is not encoded" (i.e. "sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 30:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network comprising,

- "a certification information setting unit" (i.e. "A person wishing to receive secure data generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "for generating a first certification information" (i.e. "generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "for transmitting the first certification information to the software update device" (i.e. "The encryption key is made public, while the corresponding decryption key is kept secret") [column 11 lines 29-31];
- "a certifying unit for executing a certification process, when receiving a second certification information from the software update device, by comparing the first and second certification information" (i.e. "Because the signature message can only be decrypted with the sender's public key, the recipient can use the sender's public key to confirm that the signature message originated with the sender") [column 11 lines 42-45];
- "an updating unit for receiving an update software" [Fig 10 illustrates a device to be updated];

- "for updating a software of the communication device from the software update device... when the certification process succeeds" (i.e. "As is seen in FIG. 5, update data may be obtained by providing an "image" of the data to be written to a programmable memory, for example, the programmable memory 14") [column 11 lines 18-20];
- "for updating the software of the communication device" (i.e. "FIG. 5 illustrates operations according to embodiments of the present invention for performing an update of firmware or other data stored in a programmable memory") [column 11 lines 13-15];

but they do not disclose,

- "via a second communication path"
- "the second communication path having a process load less than that of the first communication path"

however, Kidder et al. do disclose,

- "Ethernet 32 provides an out-of-band control path, meaning that control information passes over Ethernet 32 but the network data being switched by computer system 10 passes to and from external network connections 31a-31xx over a separate data path 34" [column 9 lines 14-18];
- "This external network control data is also assigned a high priority when passed over the Ethernet to ensure that it is not dropped during periods of heavy traffic on the Ethernet" [column 9 lines 20-23];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "via a second communication path" and "the second communication path having a process load less than that of the first communication path," in the invention as disclosed by Hind et al. for the purposes of transmitting authentication information and data over separate data paths for ensuring traffic quality of service.

Claim 31:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, as in Claim 30 above, further comprising,

- "a certification information invalidating unit for invalidating the first certification information subsequent to the transmittal of the update software" (i.e. "If the results do not match, then the signature is not verified (block 406) and the image is rejected, the update procedure terminated and the latch set to disable updates (block 412)") [column 12 lines 52-55].

Claim 32:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, as in Claim 30 above, further comprising,

- "a control part for instructing update of the software of the communication device" (i.e. "FIG. 5 illustrates operations according to embodiments of the present invention for performing an update of firmware or other data stored in a programmable memory") [column 11 lines 13-15].

Claim 35:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, as in Claim 30 above, further comprising,

- "the second communication path is a communication path for communicating by using FTP" (i.e. "an authorized administrator sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 36:

Hind et al. disclose a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, as in Claim 30 above, further comprising,

- "data transmitted via the first communication path is encoded" (i.e. "the image may be digitally signed or otherwise encrypted utilizing, for example, an asymmetric key cryptosystem") [column 11 lines 22-24];
- "data transmitted via the second communication path is not encoded" (i.e. "an authorized administrator sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 37:

Hind et al. disclose a software update system comprising,

- "a communication device" [Fig 10 illustrates a device used in communication with another device];
- "a software update device in communication with the communication device" [Fig 10 illustrates an updater in communication with a device used in communication with another device];
- "a certification information setting unit" (i.e. "A person wishing to receive secure data generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "for generating a first certification information" (i.e. "generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "for transmitting the first certification information to the software update device" (i.e. "The encryption key is made public, while the corresponding decryption key is kept secret") [column 11 lines 29-31];
- "a certifying unit for executing a certification process, when receiving a second certification information from the software update device, by comparing the first and second certification information" (i.e. "Because the signature message can only be decrypted with the sender's public key, the recipient can use the sender's public key to confirm that the signature message originated with the sender") [column 11 lines 42-45];
- "an updating unit for receiving an update software" [Fig 10 illustrates a device to be updated];

- "for updating a software of the communication device from the, software update device... when the certification process succeeds" (i.e. "As is seen in FIG. 5, update data may be obtained by providing an "image" of the data to be written to a programmable memory, for example, the programmable memory 14") [column 11 lines 18-20];
- "for updating the software of the communication device" (i.e. "FIG. 5 illustrates operations according to embodiments of the present invention for performing an update of firmware or other data stored in a programmable memory") [column 11 lines 13-15];
- "a memory unit for storing the first certification information" [Fig 3 illustrates a memory];
- "a certification requesting unit" [Fig 10 illustrates a device to be authenticated];
- "for transmitting the second certification information to the communication device" (i.e. "The encryption key is made public, while the corresponding decryption key is kept secret") [column 11 lines 35-39];
- "for requesting the communication device to execute the certification process with the first and second certification information" (i.e. "Because the signature message can only be decrypted with the sender's public key, the recipient can use the sender's public key to confirm that the signature message originated with the sender") [column 11 lines 42-45];
- "a transmitting unit for transmitting the update software to the communication device... when the certification process succeeds" (i.e. "As is seen in FIG. 5, update data may be obtained by providing an "image" of the data to be written to a programmable memory, for example, the programmable memory 14") [column 11 lines 18-20];

but they do not disclose,

- "via a second communication path"
- "the second communication path having a process load less than that of the first communication path"

however, Kidder et al. do disclose,

- "Ethernet 32 provides an out-of-band control path, meaning that control information passes over Ethernet 32 but the network data being switched by computer system 10 passes to and from external network connections 31a-31xx over a separate data path 34" [column 9 lines 14-18];
- "This external network control data is also assigned a high priority when passed over the Ethernet to ensure that it is not dropped during periods of heavy traffic on the Ethernet" [column 9 lines 20-23];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "via a second communication path" and "the second communication path having a process load less than that of the first communication path," in the invention as disclosed by Hind et al. for the purposes of transmitting authentication information and data over separate data paths for ensuring traffic quality of service.

Claim 38:

Hind et al. disclose a software update system, as in Claim 37 above, further comprising,

- "the communication device further has a certification information invalidating unit for invalidating the first certification information subsequent to the transmittal of the update software" (i.e. "If the results do not match, then the signature is not verified (block 406) and the image is rejected, the update procedure terminated and the latch set to disable updates (block 412)") [column 12 lines 52-55].

Claim 41:

Hind et al. disclose a software update system, as in Claim 37 above, further comprising,

- "the second communication path is a communication path for communicating by using FTP" (i.e. "an authorized administrator sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claim 42:

Hind et al. disclose a software update system, as in Claim 37 above, further comprising,

- "data transmitted via the first communication path is encoded" (i.e. "the image may be digitally signed or otherwise encrypted utilizing, for example, an asymmetric key cryptosystem") [column 11 lines 22-24];
- "data transmitted via the second communication path is not encoded" (i.e. "an authorized administrator sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claims 43 & 50:

Hind et al. disclose a software update method using a communication device capable of communicating with a software update device via a network and a program to be installed or executed by a computer for controlling a communication device capable of communicating with a software update device via a network comprising,

- "(a generating function for) generating a first certification information" (i.e. "A person wishing to receive secure data generates a pair of corresponding encryption and decryption keys") [column 11 lines 27-29];
- "(a transmitting function for) transmitting the first certification information to the software update device" (i.e. "The encryption key is made public, while the corresponding decryption key is kept secret") [column 11 lines 29-31];
- "(an executing function for) executing a certification process, when receiving a second certification information from the software update device, by comparing the first and second certification information" (i.e. "Because the signature message can only be decrypted with the sender's public key, the recipient can use the sender's public key to confirm that the signature message originated with the sender") [column 11 lines 42-45];
- "(a receiving function for) receiving an update software for updating a software of the communication device from the software update device... when the certification process succeeds" (i.e. "As is seen in FIG. 5, update data may be obtained by providing an "image" of the data to be written to a programmable memory, for example, the programmable memory 14") [column 11 lines 18-20];

- "(an updating function for) updating the software of the communication device" (i.e. "FIG. 5 illustrates operations according to embodiments of the present invention for performing an update of firmware or other data stored in a programmable memory") [column 11 lines 13-15];

but they do not disclose,

- "via a second communication path"
- "the second communication path having a process load less than that of the first communication path"

however, Kidder et al. do disclose,

- "Ethernet 32 provides an out-of-band control path, meaning that control information passes over Ethernet 32 but the network data being switched by computer system 10 passes to and from external network connections 31a-31xx over a separate data path 34" [column 9 lines 14-18];
- "This external network control data is also assigned a high priority when passed over the Ethernet to ensure that it is not dropped during periods of heavy traffic on the Ethernet" [column 9 lines 20-23];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "via a second communication path" and "the second communication path having a process load less than that of the first communication path," in the invention as disclosed by Hind et al. for the purposes of transmitting authentication information and data over separate data paths for ensuring traffic quality of service.

Claims 44 & 51:

Hind et al. disclose a software update method using a communication device capable of communicating with a software update device via a network and a program to be installed or executed by a computer for controlling a communication device capable of communicating with a software update device via a network, as in Claims 43 & 50 above respectively, further comprising,

- "a step/function of invalidating the first certification information subsequent to the transmittal of the update software" (i.e. "If the results do not match, then the signature is not verified (block 406) and the image is rejected, the update procedure terminated and the latch set to disable updates (block 412)") [column 12 lines 52-55].

Claims 45 & 52:

Hind et al. disclose a software update method using a communication device capable of communicating with a software update device via a network and a program to be installed or executed by a computer for controlling a communication device capable of communicating with a software update device via a network, as in Claims 43 & 50 above respectively, further comprising,

- "a step/function of updating the software in response to an instruction to update the software from a control part" (i.e. "FIG. 5 illustrates operations according to embodiments of the present invention for performing an update of firmware or other data stored in a programmable memory") [column 11 lines 13-15].

Claims 48 & 55:

Hind et al. disclose a software update method using a communication device capable of communicating with a software update device via a network and a program to be installed or executed by a computer for controlling a communication device capable of communicating with a software update device via a network, as in Claims 43 & 50 above respectively, further comprising,

- "the second communication path is a communication path for communicating by using FTP" (i.e. "an authorized administrator sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

Claims 49 & 56:

Hind et al. disclose a software update method using a communication device capable of communicating with a software update device via a network and a program to be installed or executed by a computer for controlling a communication device capable of communicating with a software update device via a network, as in Claims 43 & 50 above respectively, further comprising,

- "data transmitted via the first communication path is encoded" (i.e. "the image may be digitally signed or otherwise encrypted utilizing, for example, an asymmetric key cryptosystem") [column 11 lines 22-24];
- "data transmitted via the second communication path is not encoded" (i.e. "an authorized administrator sending a firmware file to the device via a network protocol such as Trivial File Transfer Protocol (TFTP)") [column 12 lines 4-6].

6. Claims 5, 11, 19, 27, 34, 40, 47, & 54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. (US-7069452-B1) in view of Kidder et al. (US-6880086-B2) and in further view of Raduchel et al. (US-6338138-B1).

Claims 5, 11, 19, 27, 34, 40, 47, & 54:

Hind et al. and Kidder et al. disclose a software update device capable of communicating with a target update device via a network, a couple software update systems, a software update method using a software update device capable of communicating with a target update device via a network, a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, a communication device capable of communicating with a software update device via a network, a software update method using a communication device capable of communicating with a software update device via a network, and a program to be installed or executed by a computer for controlling a communication device capable of communicating with a software update device via a network, as in Claims 1, 8, 14, 22, 30, 37, 43, & 50 above, but do not disclose,

- "the first communication path is a communication path for communicating by using SSL"

however, Raduchel et al. do disclose,

- "the authentication information, including the username and password, is sent by the browser to the authentication manager using the well-known HyperText Transfer Protocol (HTTPS), and using the well-known Secure Socket Layer (step 206)" [column 5 lines 12-16];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "the first communication path is a communication path for communicating by using SSL," in the invention as disclosed by Hind et al. and Kidder et al. since SSL is a commonly used form of authentication between devices on the Internet.

7. Claims 10, 18, 26, 33, 39, 46, & 53 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hind et al. (US-7069452-B1) in view of Kidder et al. (US-6880086-B2) and in further view of Bealkowski et al. (US-5878256-A).

Claim 10:

Hind et al. and Kidder et al. disclose a software update system, as in Claim 8 above, further comprising,

- "a version information transmitting unit for transmitting version information of the target update device in response to a request from the software update device" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];
- "the software update device further has a version information unit" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];

- "for obtaining the version information by requesting the target update device to transmit the version information when the start notification is received after the transmittal of the update software" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];
- "for confirming the update by comparing with version information of the transmitted update software" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];

but they do not disclose,

- "a restarting unit for restarting the target update device after the software is updated by the updating unit"
- "a start notification transmitting unit for transmitting a start notification informing that the target update device is started to the software update device when the target update device is started"

however, Bealkowski et al. do disclose,

- "If the update procedure was not a functional enhancement (e.g., just a maintenance release), then the system is restarted electronically, step 820. The restart, step 820, is done to activate the new code as described in FIG. 7" [column 14 lines 43-46];
- "If the update procedure was not successful, then an error indication is given, step 818, and the user can either try the procedure again or call for service" [column 14 lines 39-40];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a restarting unit for restarting the target update device after the software is updated by the updating unit" and "a start notification transmitting unit for transmitting a start notification informing that the target update device is started to the software update device when the target update device is started," in the invention as disclosed by Hind et al. and Kidder et al. since restarting devices after a firmware update is common in order to activate the new changes. It is also implied that if error indicators are given then indicators of states of success would also be given.

Claims 18 & 26:

Hind et al. and Kidder et al. disclose a software update method using a software update device capable of communicating with a target update device via a network and a program to be installed or executed by a computer for controlling a software update device capable of communicating with a target update device via a network, as in Claims 14 & 22 above respectively, further comprising,

- "obtaining version information of the software of the target update device from the target update device when the start notification is received after the transmittal of the update software" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];
- "confirming the update by comparing with version information of the transmitted update software" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];

but they do not disclose,

- "receiving a start notification informing that the target update device is started"

however, Bealkowski et al. do disclose,

- "If the update procedure was not successful, then an error indication is given, step 818, and the user can either try the procedure again or call for service" [column 14 lines 39-40];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "receiving a start notification informing that the target update device is started," in the invention as disclosed by Hind et al. and Kidder et al. since it is also implied that if error indicators are given then indicators of states of success would also be given.

Claim 33:

Hind et al. and Kidder et al. disclose a communication device capable of communicating with a software update device via a network, as in Claim 30 above, further comprising,

- "a version information transmitting unit for transmitting version information of the communication device in response to a request from the software update device after the start after the transmittal of the start notification" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];

but they do not disclose,

- "a restarting unit for restarting the communication device after the software is updated"
- "a start notification transmitting unit for transmitting a start notification informing that the communication device is started to the software update device when the communication device is started"

however, Bealkowski et al. do disclose,

- "If the update procedure was not a functional enhancement (e.g., just a maintenance release), then the system is restarted electronically, step 820. The restart, step 820, is done to activate the new code as described in FIG. 7" [column 14 lines 43-46];
- "If the update procedure was not successful, then an error indication is given, step 818, and the user can either try the procedure again or call for service" [column 14 lines 39-40];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a restarting unit for restarting the communication device after the software is updated" and "a start notification transmitting unit for transmitting a start notification informing that the communication device is started to the software update device when the communication device is started," in the invention as disclosed by Hind et al. and Kidder et al. since it is also implied that if error indicators are given then indicators of states of success would also be given.

Claim 39:

Hind et al. and Kidder et al. disclose a software update system, as in Claim 37 above respectively, further comprising,

- "a version information transmitting unit for transmitting version information of the communication device in response to a request from the software update device" (i.e. "these rules may refer to values which are part of the new image (for example the image

version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];

- "the software update device further has a version information unit" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];
- "for obtaining the version information by requesting the communication device to transmit the version information when the start notification is received after the transmittal of the update software" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];
- "for confirming the update by comparing with version information of the transmitted update software" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];

but they do not disclose,

- "a restarting unit for restarting the communication device after the software is updated"
- "a start notification transmitting unit for transmitting a start notification informing that the communication device is started to the software update device when the communication device is started"

however, Bealkowski et al. do disclose,

- "If the update procedure was not a functional enhancement (e.g., just a maintenance release), then the system is restarted electronically, step 820. The restart, step 820, is done to activate the new code as described in FIG. 7" [column 14 lines 43-46];
- "If the update procedure was not successful, then an error indication is given, step 818, and the user can either try the procedure again or call for service" [column 14 lines 39-40];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "a restarting unit for restarting the communication device after the software is updated" and "a start notification transmitting unit for transmitting a start notification informing that the communication device is started to the software update device when the communication device is started," in the invention as disclosed by Hind et al. and Kidder et al. since it is also implied that if error indicators are given then indicators of states of success would also be given.

Claims 46 & 53:

Hind et al. and Kidder et al. disclose a software update method using a communication device capable of communicating with a software update device via a network and a program to be installed or executed by a computer for controlling a communication device capable of communicating with a software update device via a network, as in Claims 43 & 50 above respectively, further comprising,

- "(a transmitting function for) transmitting version information of the communication device in response to a request from the software update device after the start after the transmittal of the start notification" (i.e. "these rules may refer to values which are part of the new image (for example the image version or date, range of MAC addresses, etc.), part of the active flash image, and/or values in ROM (for example, the manufacturer, model, adapter MAC or serial number, or other criteria for application of the update image") [column 15 lines 12-17];

but they do not disclose,

- "(a restarting function for) restarting the communication device after the software is updated"
- "(a transmitting function for) transmitting a start notification informing that the communication device is started to the software update device when the communication device is started"

however, Bealkowski et al. do disclose,

- "If the update procedure was not a functional enhancement (e.g., just a maintenance release), then the system is restarted electronically, step 820. The restart, step 820, is done to activate the new code as described in FIG. 7" [column 14 lines 43-46];
- "If the update procedure was not successful, then an error indication is given, step 818, and the user can either try the procedure again or call for service" [column 14 lines 39-40];

Therefore, it would have been obvious for one of ordinary skill in the art at the time of the applicant's invention to include, "(a restarting function for) restarting the communication device after the software is updated" and "(a transmitting function for) transmitting a start notification informing that the communication device is started to the software update device when the communication device is started," in the invention as disclosed by Hind et al. and Kidder et al. since it is also implied that if error indicators are given then indicators of states of success would also be given.

Conclusion

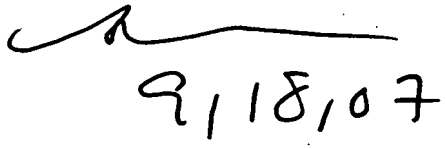
8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Examiner Oscar Louie whose telephone number is 571-270-1684. The examiner can normally be reached Monday through Thursday from 7:30 AM to 4:00 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami, can be reached at 571-272-4195. The fax phone number for Formal or Official faxes to Technology Center 2100 is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

OAL
09/18/2007

Nasser Moazzami
Supervisory Patent Examiner



9/18/07